DoD's IAVA Process

Helping Mitigate Network Security Risk to the Defense Information Infrastructure

LT Beth A. Evans, USN
DISA DoD CERT

> "Establishing trust in a highly distributed, network-centric computing environment is a fundamental issue today for the Department of Defense and its Defense Information Infrastructure (DII). Widely known and documented vulnerabilities exist throughout the networks and because of our increasing reliance on networks, these vulnerabilities have the capacity to severely degrade our operational readiness and therefore endanger national security. We must shift the current view that information assurance/systems security concerns are secondary considerations to core readiness issues. Everyone—from the highest senior levels of management to the soldiers and office workers—must understand their responsibility as a stakeholder in the vitality and security of our information systems."
>
> —Dr. John Hamre, Deputy Secretary of Defense

The Department of Defense (DoD) Computer Emergency Response Team (CERT), a branch within the Defense Information Systems Agency (DISA), is responsible for providing information assurance procedures and guidance to the DoD community for protection of the Defense Information Infrastructure (DII). Accordingly, the Deputy Secretary of Defense instituted a notification process in 1998 known as the Information Assurance Vulnerability Alert (IAVA) process and designated DISA as its manager. The IAVA process was created because DoD recognized the need for the Commanders-in-Chief (CINC), Services, and Agencies (C/S/A) to have a positive control mechanism to ensure that their system administrators received, acknowledged, and complied with vulnerability alert notifications and to ensure that corrective actions were taken against new and critical vulnerabilities.

IAVA is a Web-based process that incorporates identification and evaluation of new vulnerabilities, disseminates technical responses, and tracks compliance within the DoD community. As the IAVA process manager, DISA is responsible for disseminating the vulnerability notifications to C/S/A points of contact and providing an automated means for the points of contact to report receipt of and compliance with the alerts.

Managing the IAVA Process

DoD CERT has created a three-tiered "vulnerability hierarchy" for notifications. The first-tier notification, an alert or IAVA, is disseminated when DoD CERT documents a new vulnerability that poses an immediate, potentially severe threat to DoD systems. The IAVA requires that C/S/As report both receipt of the alert (after disseminating it to subordinate organizations) and their compliance with the corrective action(s).

The second-tier notification, a bulletin or IAVB, addresses new vulnerabilities that do not pose an immediate threat to DoD systems, but are significant enough that noncompliance with the corrective action could escalate the threat. Like the IAVA, the IAVB requires C/S/As to report receipt of the bulletin, but compliance reporting is not required (compliance requirements and decisions are made by the local commander). However, the IAVB must be disseminated down to the system administrator level within the organization.

The third-tier notification, the technical advisory, is generated when new vulnerabilities exist but are generally categorized as low risk. Potential escalation of these vulnerabilities is deemed unlikely, but the advisories are issued so that any risk of escalation in the future can be mitigated. Reporting is not required in response to a technical advisory.

The IAVA process allows waivers of the required compliance actions to be granted in response to a specific alert. Waivers are reviewed and granted by a C/S/A's Designated Approval Authority (DAA). The DAA must consider the risks involved, to both the local network and the greater DII, when granting a waiver.

Determining Notification Type

The DoD CERT learns of new vulnerabilities through incidents reported to DoD and civilian CERTs, public Internet resources, and vendor notifications. On notification of a new vulnerability, DoD CERT assesses the threat that the vulnerability poses to the DII using criteria such as the type of operating system and infrastructure affected by the exploit, the access gained by the exploit, the number of exploits reported, and the nature of the exploit's potential end result (denial of service, for example).

After the initial evaluation, a request for comments is sent to a coordination team consisting of the Joint Task Force–Computer Network Defense, Service CERTs, and joint system program managers. This team provides input in determining the type of notification to be generated. After coordination, the notification is disseminated in a variety of ways. Record message traffic (Automatic Digital Network [AUTODIN] and Defense Message System [DMS]) is sent releasing an IAVA or IAVB to the C/S/A points of contact. The message is primarily for notification purposes, as well as assignment of reporting timelines. The message directs recipients to the DoD CERT Web site (http://www.cert.mil) for technical specifics and corrective action(s). An E-mail containing the technical information is also disseminated to all IAVA list serve addressees for the IAVA, IAVB, and technical advisories. List registration can be requested by sending an E-mail to cert@cert.mil. Dissemination is restricted to .mil and .gov domains.

The reporting of receipt, compliance, and waiver information is accomplished via the unclassified or classified IAVA Web site. Normal reporting timelines are 5 days for reporting receipt (IAVA and IAVB) and 30 days for reporting compliance (IAVA). Significant progress is being made in the automation of receipt acknowledgement and compliance reporting, and as of October 1, 1999 C/S/As have access to a greatly improved utility, providing a more robust and effective automated mechanism to report their status information.

LT Beth A. Evans, USN is the Technical Analysis Division Chief for the DoD Computer Emergency Response Team, Defense Information Systems Agency, Arlington, Va. She received her B.S. in Business Administration from the University of California, Berkeley, CA in December 1990. LT Evans is currently pursuing her M.S. in Information Systems from George Mason University, Fairfax, Va. She may be reached at evansb@ncr.disa.mil.

The following vulnerabilities were addressed in the alerts and bulletins disseminated by the end of July 1999.

Alerts

1999-0001
Mountd Remote Buffer Overflow Vulnerability

1999-0002
TCP Wrappers Trojan

1999-0003
Remote FTP Vulnerability

1999-0004
Microsoft IIS "Malformed FTP List Request" Vulnerability

1999-0005
Worm.ExploreZip

1999-0006
Statd and Automountd Vulnerabilities

1999-0007
Internet Information Server (IIS) 4.0 Vulnerability

1999-0008
Calendar Manager Service Daemon Vulnerability

Bulletins

1999-0001
Cold Fusion Application Server Vulnerabilities

1999-0002
SGI Array Services Default Configuration Vulnerability